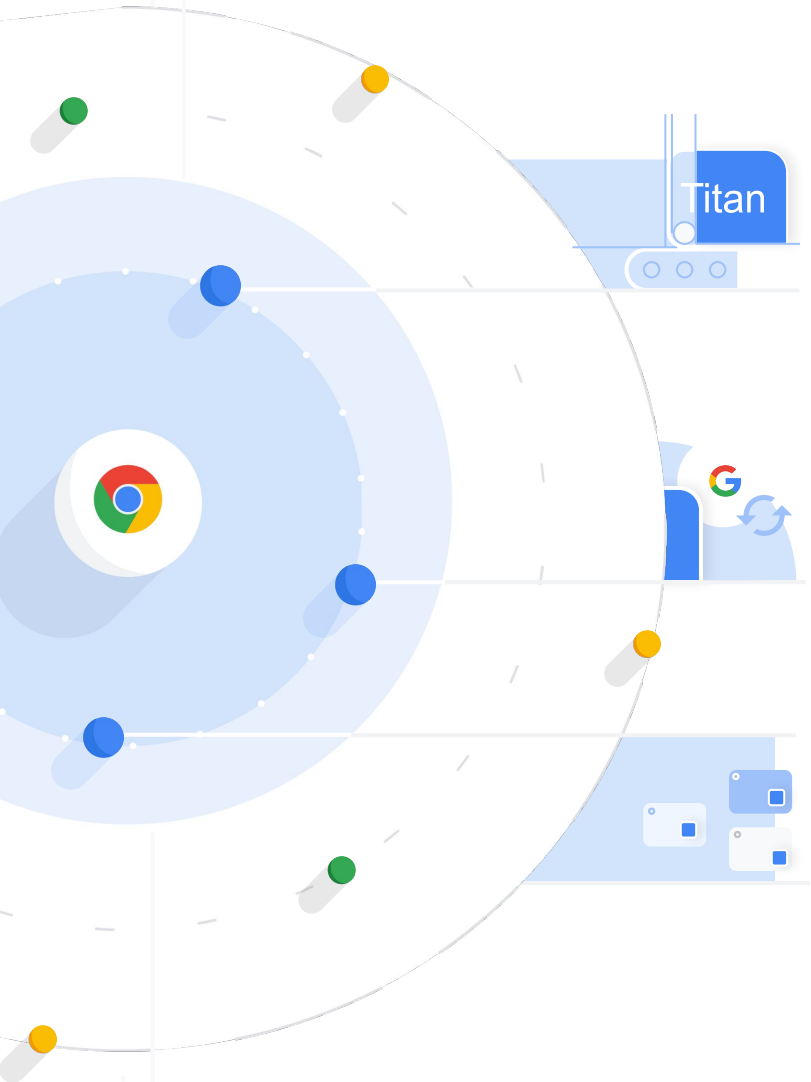
chromeOS

Titan C
信頼の基盤

Titan C は、Google が設計した ChromeOS デバイスのセキュリティ チップで*、デバイスを内側から安全に守り、ユーザーの個人情報を保護し、システムの整合性を確保します。



切れ目のないセキュリティ

Google による設計

Titan C チップの設計はすべて Google が手がけており、製造プロセスをモニタリングして品質を確保しています。製造されたチップは工場に出荷され、Chrome デバイスに組み込まれます。

Google によるアップデート

Titan C チップのファームウェア アップデートはすべて Google が提供しています。セキュリティの侵害が報告された場合も、解決策を特定してすぐにすべての Chromebook に修正プログラムが配布されるので安心です。

Chromebook に標準搭載

Titan C チップは、すべての価格帯の Chromebook に搭載されています。常時動作しているため、設定して有効にする必要はありません。

*2019 年 1 月以降に販売された、Lenovo 100e Chromebook 2nd Gen MTK と Lenovo 300e Chromebook 2nd Gen MTK を除くすべての Chromebook に、Titan セキュリティ チップが搭載されています。上記の 2 機種には別のセキュリティ チップが搭載されています。

ユーザーの保護

遠隔ハードウェアでのログイン試行を防ぐ

Titan C はユーザーデータ暗号鍵へのアクセスを保護します。パスワードやハードドライブがハッカーの手に渡っても、別のデバイスを使ってデータを復号できないようになっています。

パスワードの総当たり攻撃から守る

Titan C は総当たり攻撃からデバイスを保護します。ハッカーが何百万通りもパスワードや PIN コードの組み合わせを試して、デバイスにログインしようとしても阻止します。

フィッシング攻撃から保護する

Titan C では 2 段階認証が有効になっており、パスワードを入力して電源ボタンを押さなければデバイスにログインできません。

システムの整合性

不正な改ざんから OS やファームウェアを守る

Titan C は確認付きブートのプロセスをサポートし、不正なコードによる ChromeOS の改ざんを防ぎます。

企業のポリシー違反を防ぐ

Titan C は、Chrome Enterprise で設定した多数のポリシー（デバイスのデベロッパー モードへの切り替えを無効にするなど）を管理対象の Chromebook に適用するのにも役立ちます。

不正使用されたデバイスでのアプリへのアクセスを阻止する

アプリのサードパーティ デベロッパーは、Titan C の「確認済みアクセス」機能を使用して、アプリへのアクセスに使用されているデバイスとそのデータが不正使用されていないことを確認できます。

chromeOS

ChromeOS の
セキュリティについて
詳しくは、ドキュメントをダウンロードして
ご確認ください